**Microsoft 365 Collaboration Apps Best Practices**

20This resource corresponds to the **Microsoft 365 Collaboration Apps Best Practices Checklist** and is intended to be used as a baseline for provisioning new Microsoft 365 tenants according to best practices.

© Copyright 2019-2022

1

© Copyright 2019-2022

2

Table of Contents

[**Microsoft 365 Collaboration Apps Best Practices**](#_bookmark0)[1](#_bookmark0)

[**Change Log**](#_bookmark1)[2](#_bookmark1)

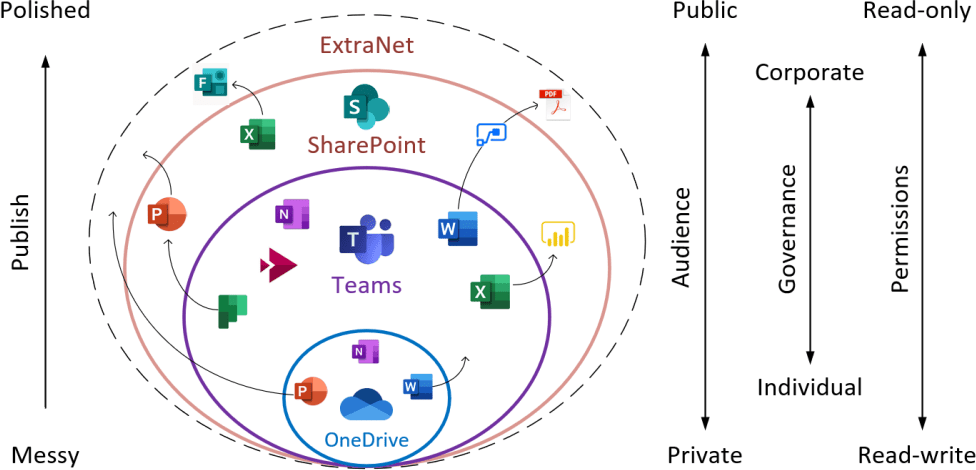
[**Spheres of Collaboration and Governance**](#_bookmark2)[4](#_bookmark2)

* [**Configure external collaboration settings**](#_bookmark3)[4](#_bookmark3)
* [**Configure governance options for Groups**](#_bookmark4)[6](#_bookmark4)
* [**Guest access in Teams**](#_bookmark5)[7](#_bookmark5)
* [**External access in Teams**](#_bookmark6)[8](#_bookmark6)
* [**External storage in Teams**](#_bookmark7)[8](#_bookmark7)
* [**Messaging, Meetings and Live events settings & policies**](#_bookmark8)[9](#_bookmark8)
* [**Manage apps and app policies in Teams**](#_bookmark9)[10](#_bookmark9)
* [**Enable or disable Private channels**](#_bookmark10)[12](#_bookmark10)
* [**Using Policy packages**](#_bookmark11)[13](#_bookmark11)
* [**Global Sharing settings in OneDrive and SharePoint**](#_bookmark12)[15](#_bookmark12)
* [**Site-level sharing settings**](#_bookmark13)[17](#_bookmark13)
* [**Customize Access Control for SharePoint Online and OneDrive for Business**](#_bookmark14)[18](#_bookmark14)
* [**Use “Anchor” teams in Microsoft Teams**](#_bookmark15)[20](#_bookmark15)
* [**Use Communication Sites for custom permissions**](#_bookmark16)[21](#_bookmark16)

[**Conclusion**](#_bookmark17)[22](#_bookmark17)

© Copyright 2019-2022

3



**Spheres of Collaboration and Governance**

Microsoft 365 is built on three primary “spheres” of collaboration:

•

**OneDrive**: Individual sphere, where you keep your own content and work alone or with just a small handful of others, invited as needed to individual files.

**Teams**: The “team” sphere, where you work in small groups to accomplish bigger goals or projects involving multiple files.

**SharePoint**: The “everyone” sphere, often used to distribute finished content out to

wider audiences, or as a place for company-wide file repositories.

•

•

It is possible to customize or “govern” these applications for your organization’s unique collaboration needs. The dirty little secret here is that *there is no Best Practice*—how an organization chooses to shape their information architecture and the boundaries they set around collaboration is largely up to them. Even though there is no “Best Practice” per se, note that it is still possible to end up with a “Wrong Practice”—and that is by failing to discuss the possibilities with the stakeholders and decision makers in the first place!

The controls being discussed in the following pages are not listed in any particular order within this guide (i.e., they are not ranked by relative importance).

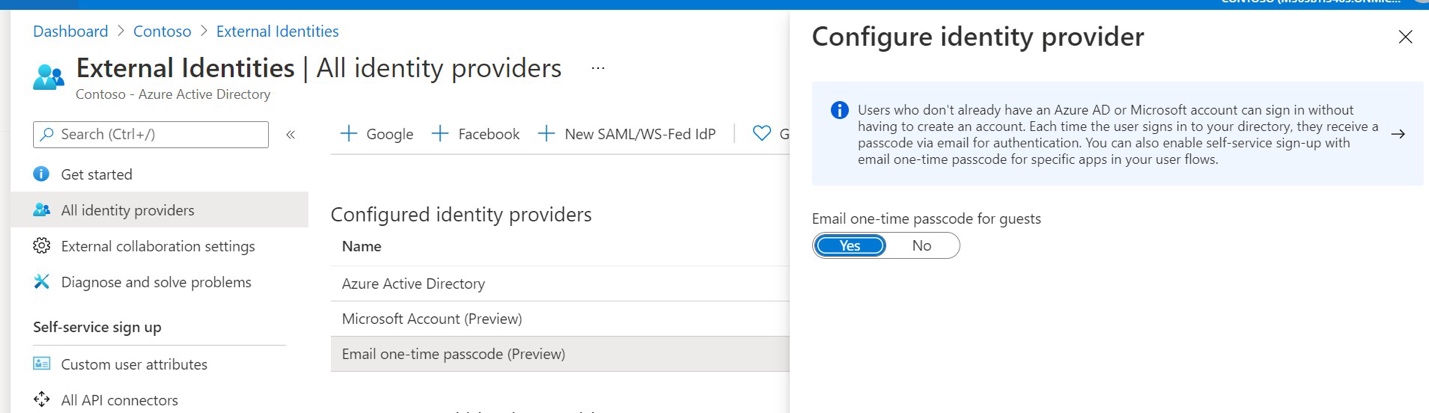
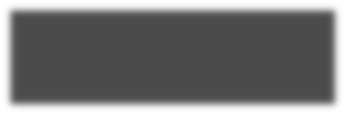
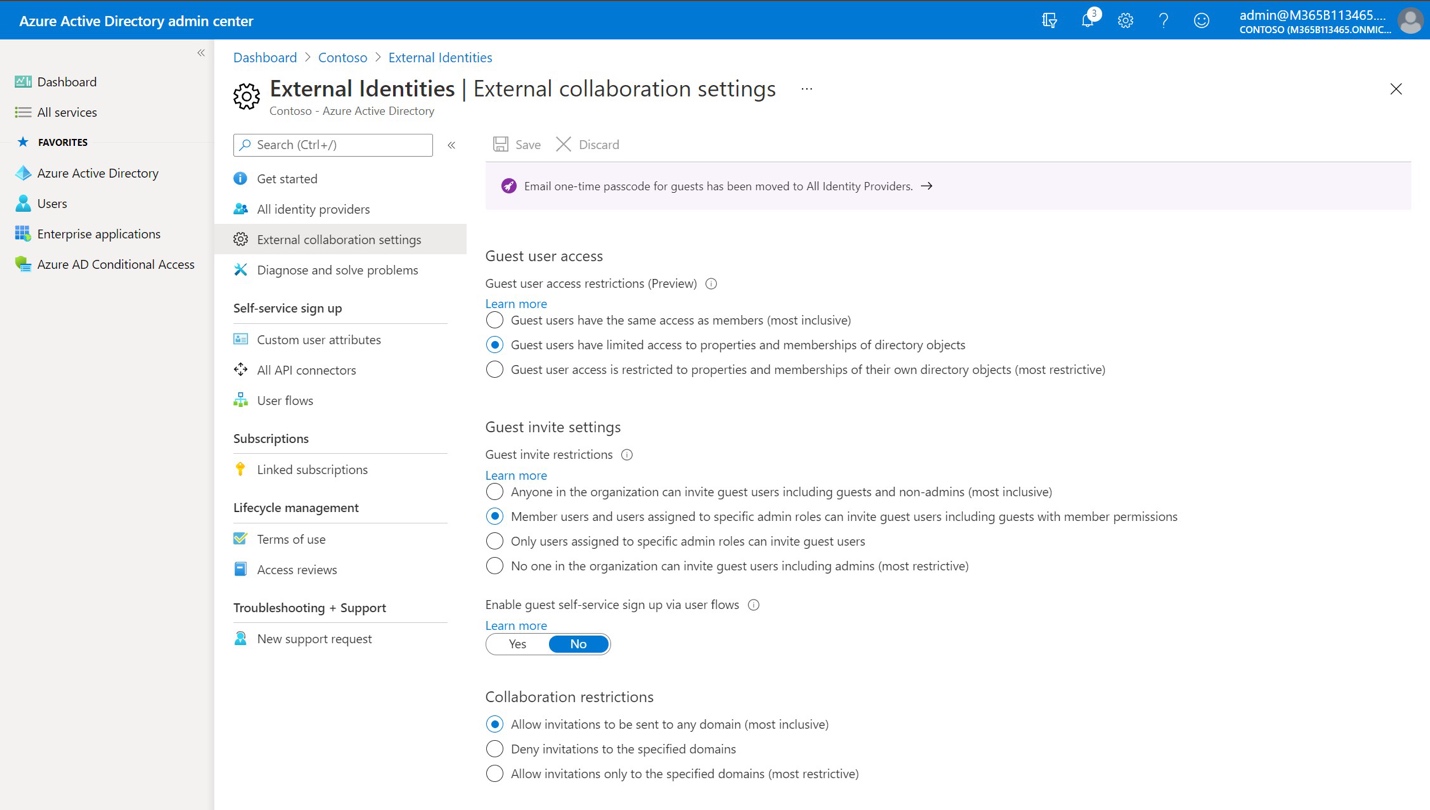
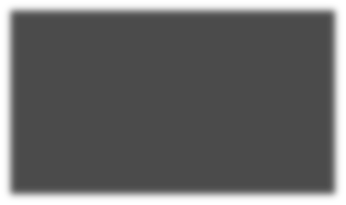
* **Configure external collaboration settings**

You can get more granular with your external collaboration settings at the service level (e.g.,

SharePoint admin center), but there is one place want to highlight, and this would impact all services globally: **Azure AD > External Identities > External collaboration settings**.

© Copyright 2019-2022

4



Guests are users outside of the organization who have been invited to collaborate on resources. Most people are happy to share certain content with partners and customers outside of their own organization, but very rarely do they want those people turning around and sharing out or inviting *other guests* to that same content. As well, they may want guests to have more limited access to the directory than their own internal users.

This may not always be true for every business, but what have depicted above is very often the preferred configuration. If you want to further limit invitations you can use this page to do so.

You will notice also that it is possible to restrict guest access by domains at the bottom of the

page, which is rarely used, but where it is required, you will need to include it in your implementation, as well.

© Copyright 2019-2022

5

Under **All identity providers**, you should click **Enable Email One-Time Passcode** for guests (Preview). This setting turns on secure, time-bound passcodes (expiry after 30 minutes) that will make life easier for guests who do not have a Microsoft account. This may be enabled by default

in the future, but you will want to double check on it for each new tenant you configure.

* **Configure governance options for Groups**

will call attention to two governance options related to Microsoft 365 Groups that think are worth considering with every deployment, which impact many services in Office 365 such as Outlook, Teams, SharePoint, and Planner.

**Group creation**: The ability to create a Microsoft 365 Group and all the associated content (e.g., SharePoint Site Collection, email address/group mailbox, etc., etc.) opens a can of worms for some people. Restrict this too much and it can be hard to get certain tasks done. Restrict it too little and you can end up with some serious clutter / sprawl. Limiting the creation of groups to a specific security group called “Group Creators” may be a good balance, with approved content creators or power users who can be responsive to requests and are on top of the whole data management thing.

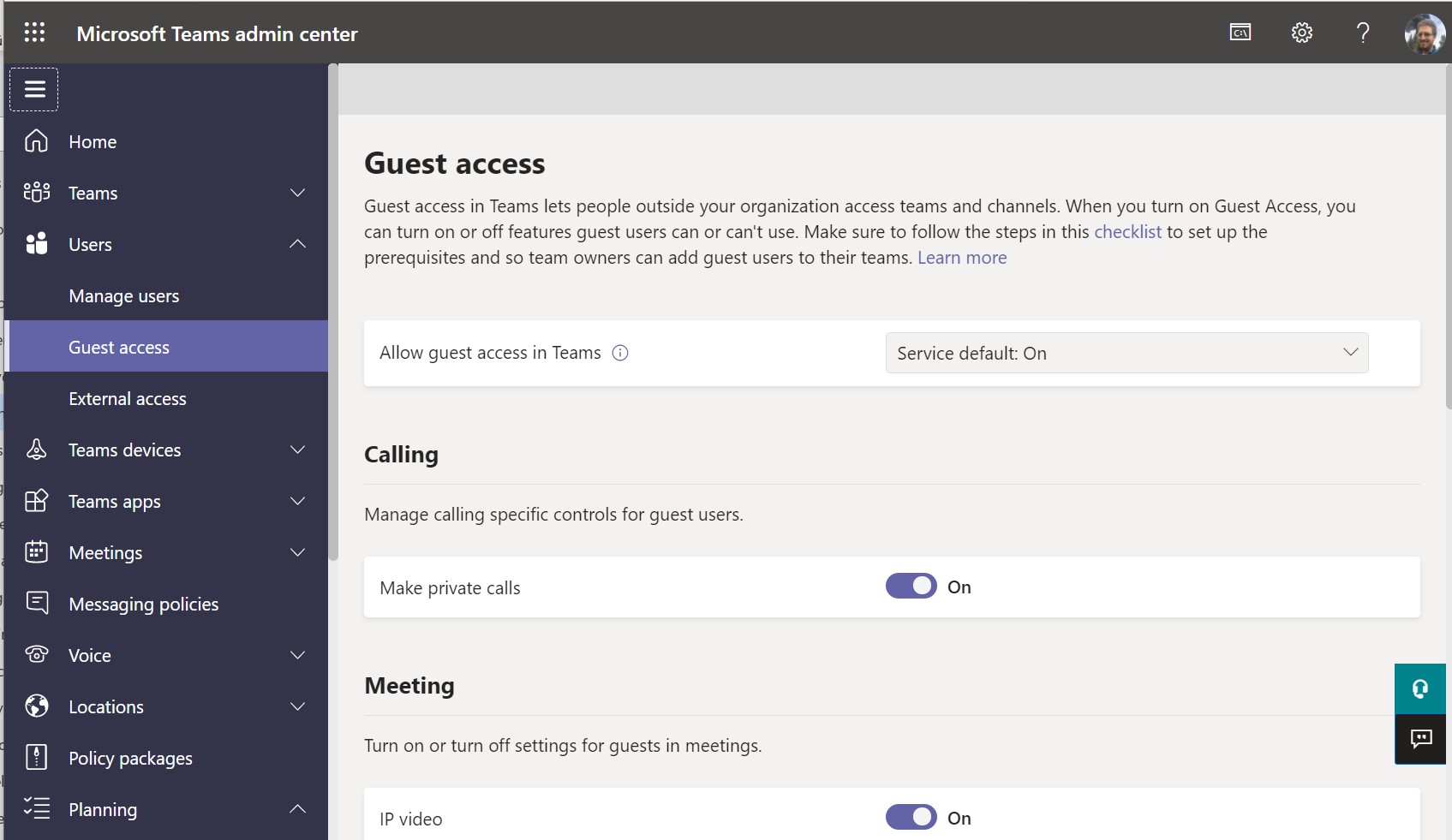
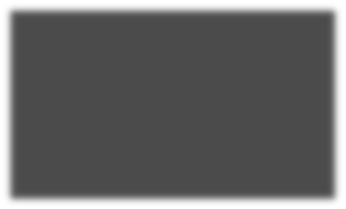
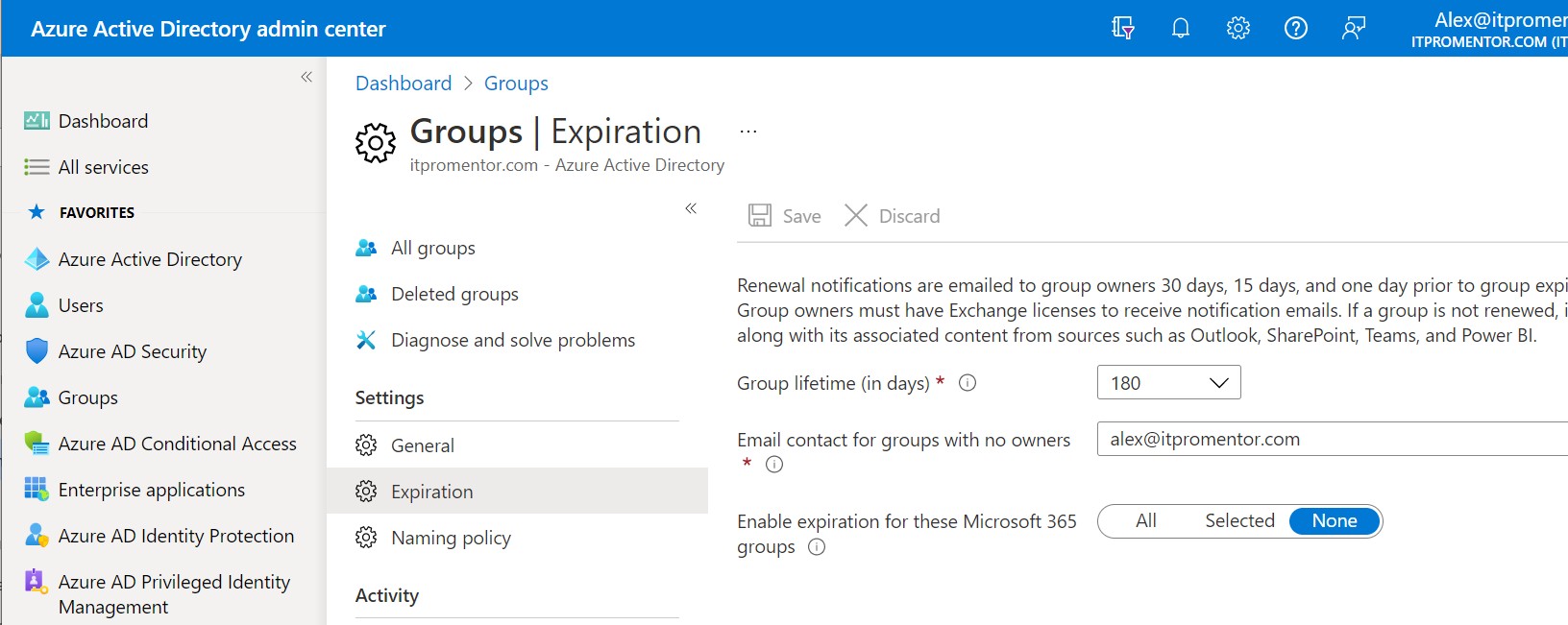
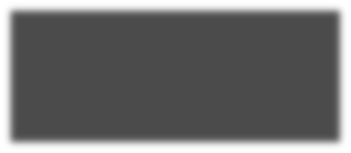
[Follow the steps in this article](https://docs.microsoft.com/en-us/office365/admin/create-groups/manage-creation-of-groups?view=o365-worldwide) if you need to restrict the capability using a security group. have a [script on GitHub](https://github.com/vanvfields/Microsoft-365/blob/master/Azure%20AD/Limit-GroupsCreation.ps1) as well; all you have to do is specify the name of the security group you will use for Group creators at the beginning of the script.

**Expiration:** Many groups that are created, for example via the Microsoft Teams application, are temporary in nature. Therefore, it is a good practice to enable an expiration policy, which notifies the group owner(s) regularly about the upcoming expiration of their groups and gives them the chance to extend the life of the group, or let it fade into dust via expiration (read: deletion).

Go to **Azure Active Directory > Groups > Expiration**. You can define a Group lifetime (in days), as well as an email contact for groups without owners (e.g., Owners who have since departed the organization).

© Copyright 2019-2022

6



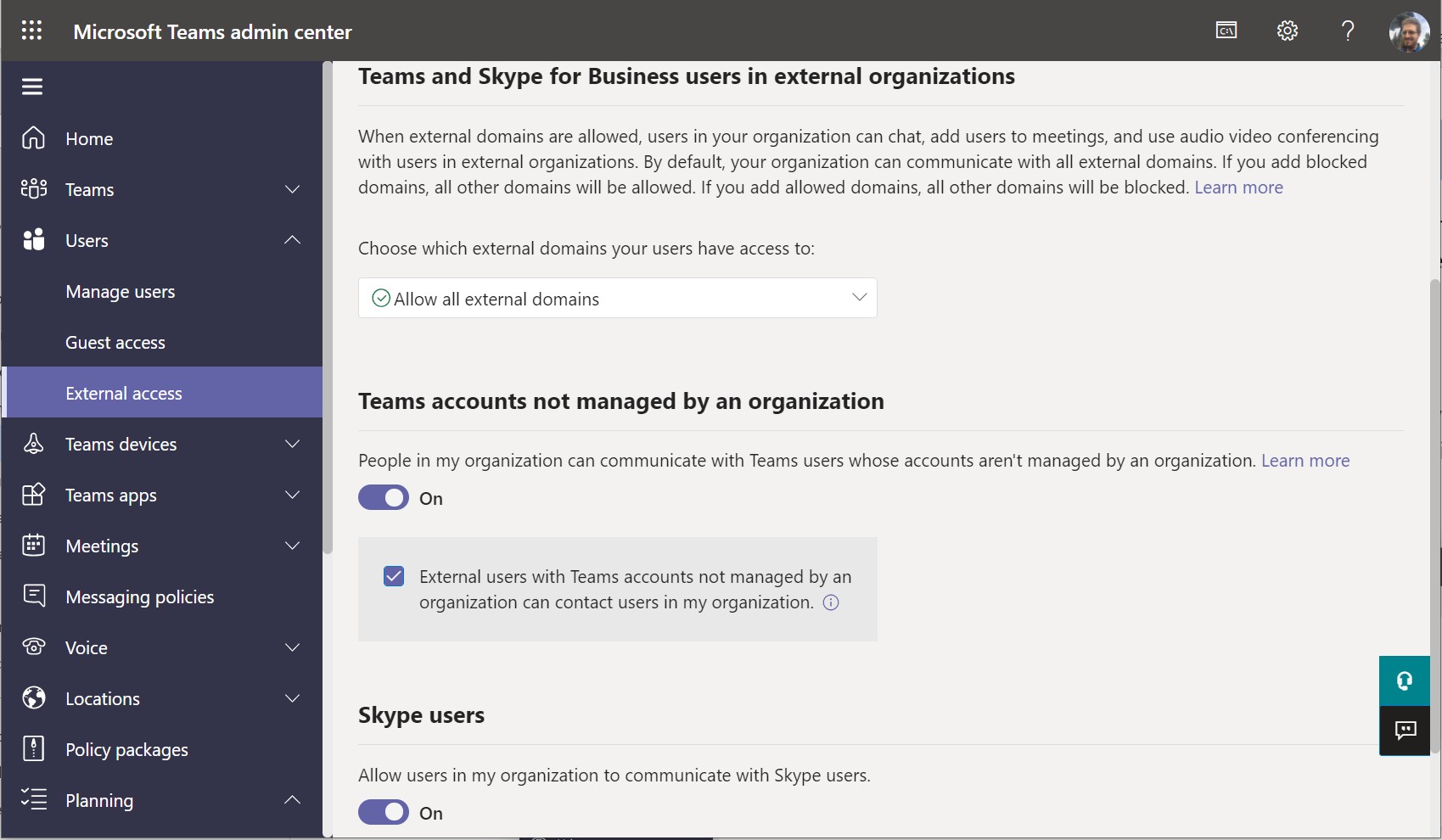
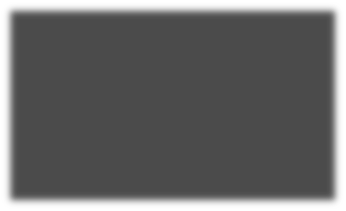
There are other options for Groups here as well—explore them under the **General** and **Naming policy blades**. But *Creation* and *Expiration* are the top two, usually.

* **Guest access in Teams**

Decide whether members should be able to invite external users into Teams for collaboration purposes. **Teams admin center > Users > Guest access**.

© Copyright 2019-2022

7



If you enable this globally, know that it is also possible to disable this on individual Teams using a Sensitivity label—for example, a Team that should remain “Confidential” would receive the

appropriate classification via Sensitivity Label.

* **External access in Teams**

External access refers to Chat functionality—and whether users should be able to chat with other Teams or Skype users outside of their own organization. **Teams admin center > Users >**

**External access**.

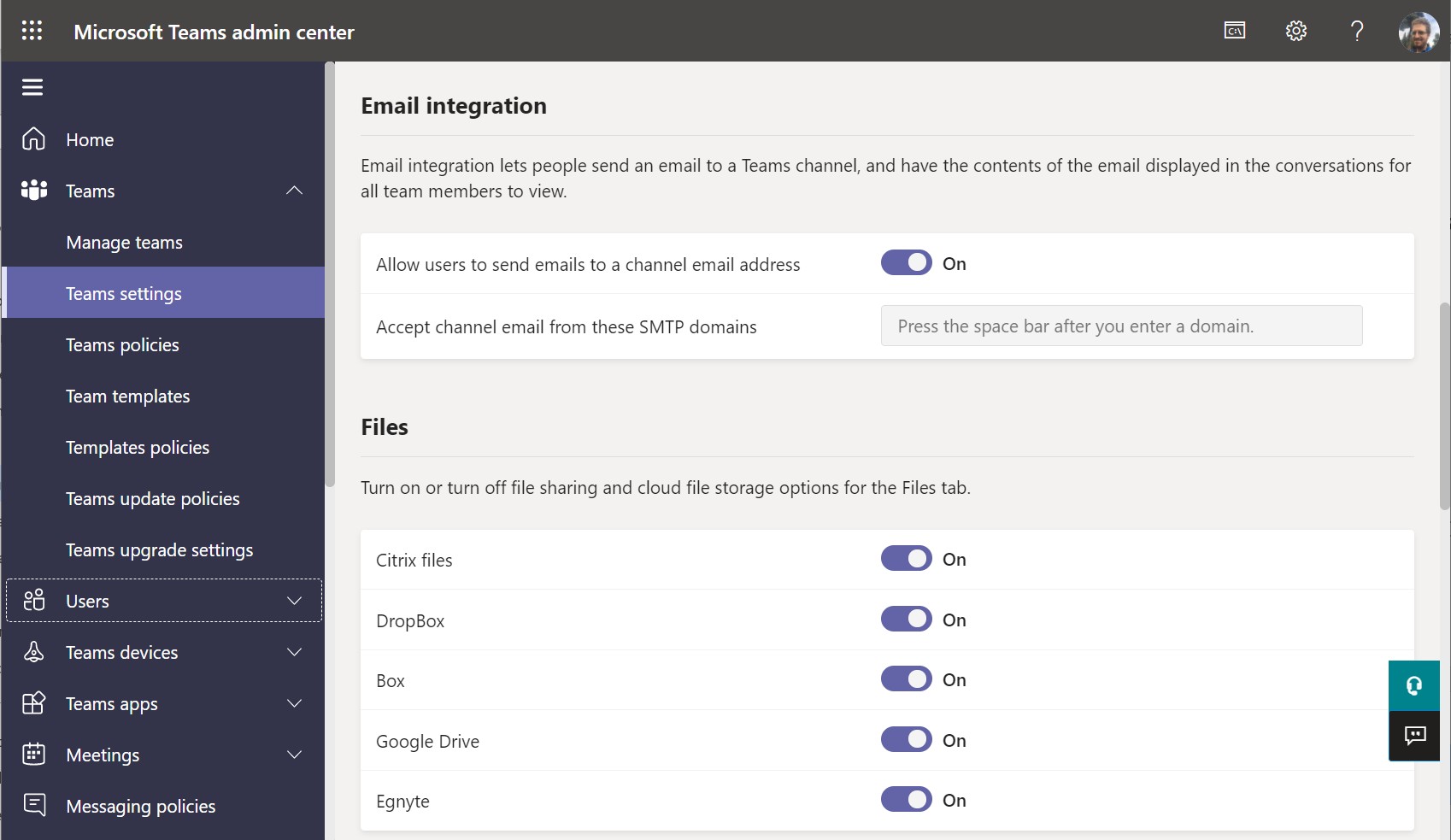
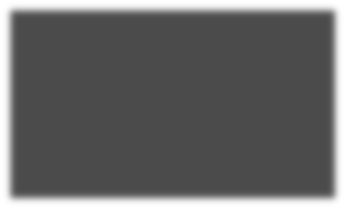
You can restrict this by domain or just disable it (if there is no intention to allow chat communication with external parties).

* **External storage in Teams**

By default, users can attach outside storage locations such as DropBox and GSuite to Teams channels. **Teams admin center > Teams > Teams settings > Files**.

© Copyright 2019-2022

8



If you disable these providers, users will only be able to store and share files within the managed Microsoft 365 environment. You should also review the other settings under **Teams settings**.

* **Messaging, Meetings and Live events settings & policies**

You will want to review the default global settings and policies around messaging, meetings, and live events. Note that *settings* are global, while *policies* can be assigned to specific groups of users. However, there are “Global policies” which contain settings that are applied if no other specific policy is applied.

From the Teams admin center, be sure to review the settings in each of the following:

Messaging policies > Global

Meetings > Meetings policies > Global Meetings > Live events policies> Global Meetings > Meeting settings

Meetings > Live event settings

•

•

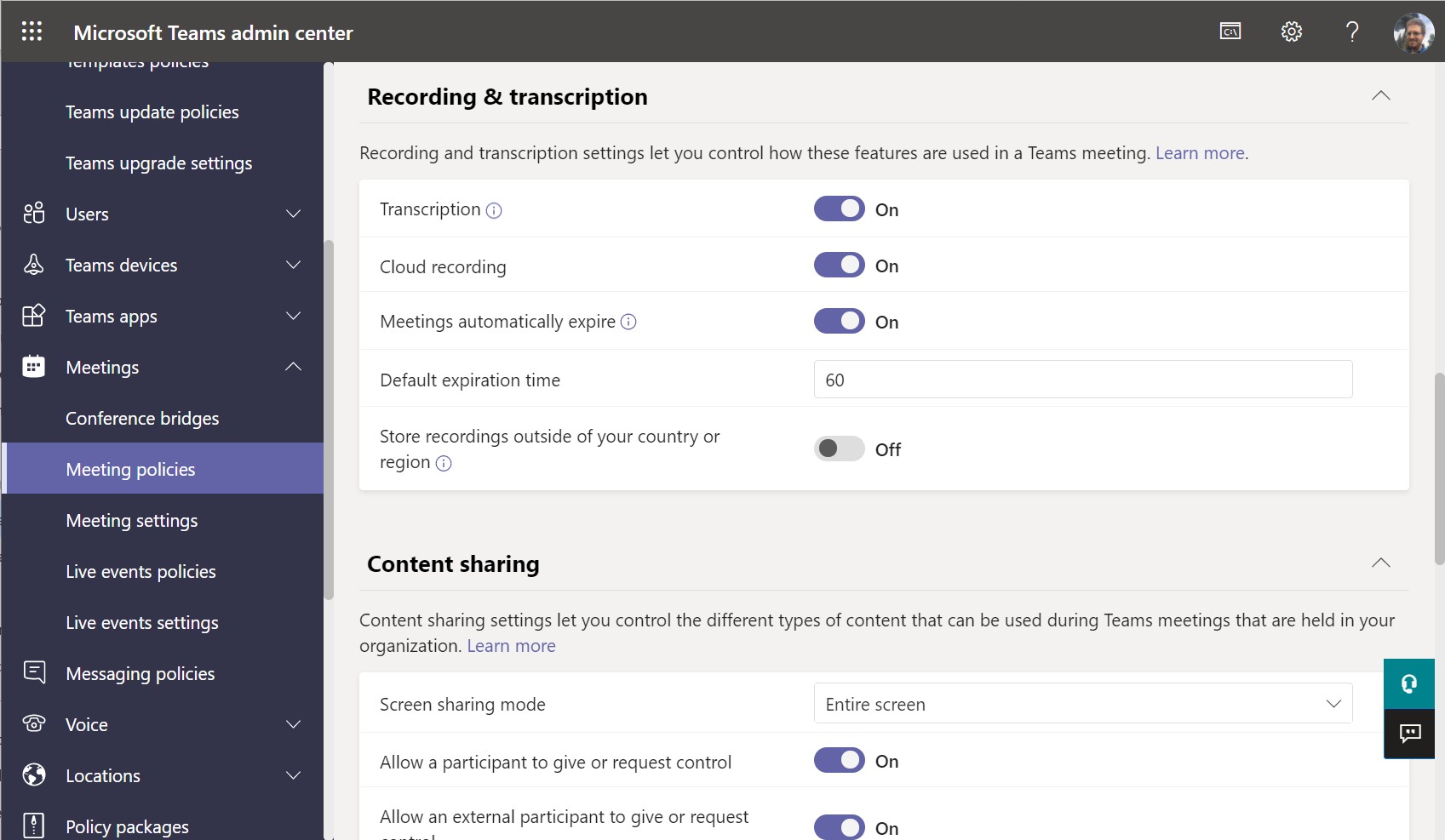
•

•

•

© Copyright 2019-2022

9



You can refer to the Governance Workbook to see all of the settings and policies for your default configuration. Most organizations will accept the defaults in most cases, but you should

ensure the settings meet your requirements, or create your own custom policies.

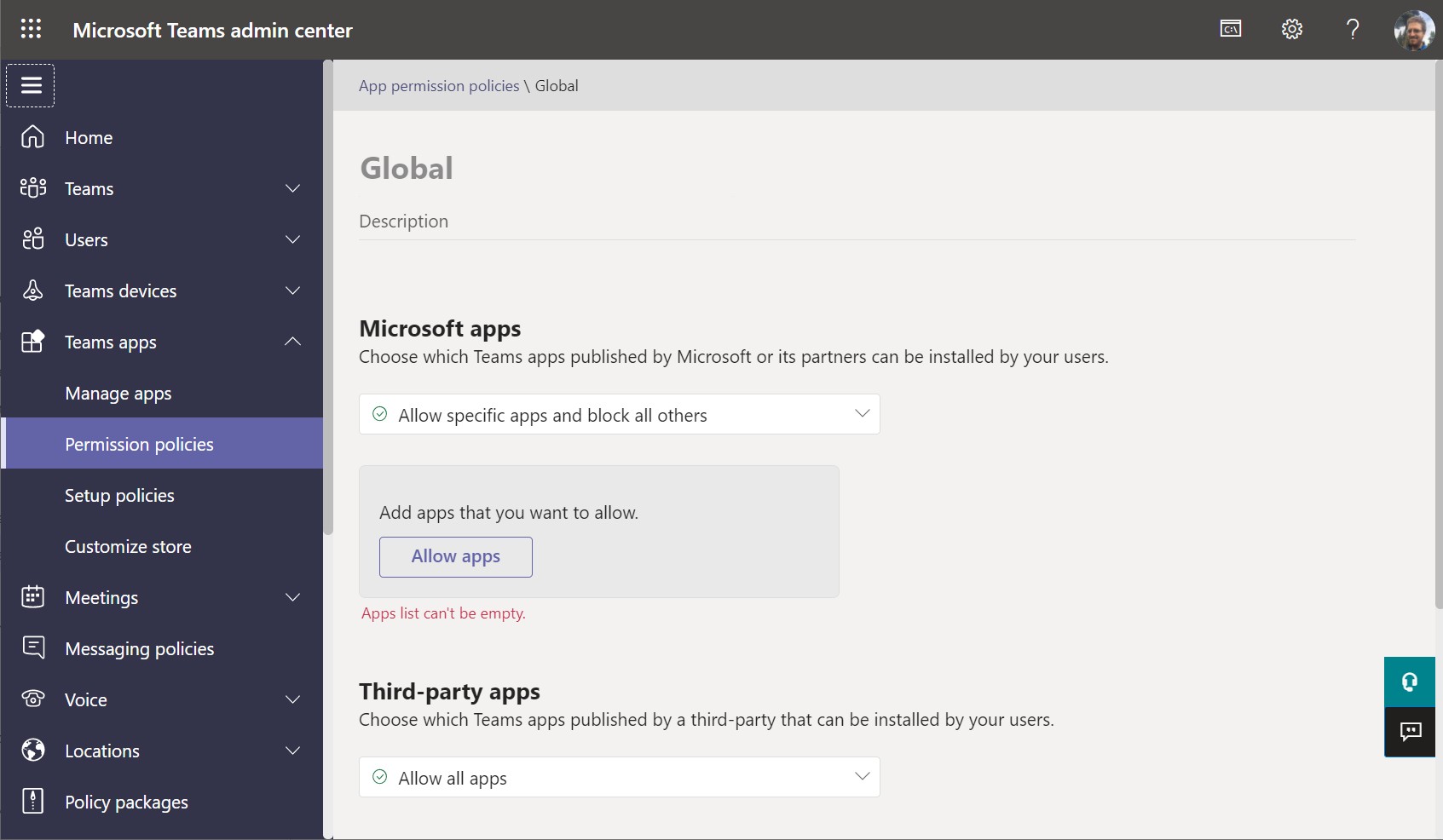
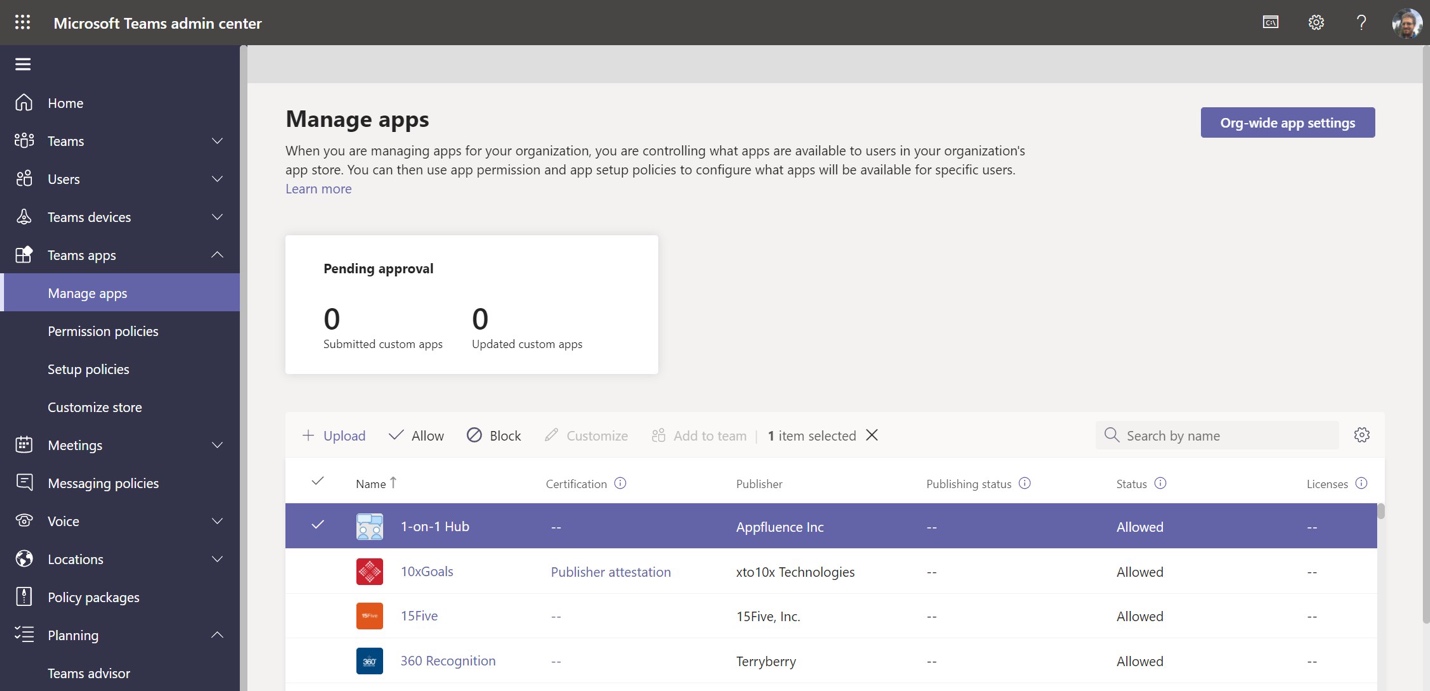
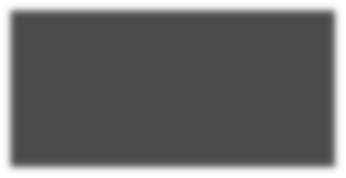
* **Manage apps and app policies in Teams**

From **Teams apps > Manage apps**, you can **Allow** or **Block** specific apps in the Teams app store, or use the **Org-wide app settings** if you want to block all apps wholesale (almost always

disable custom apps, since this is not typically something SMB customers require).

© Copyright 2019-2022

10



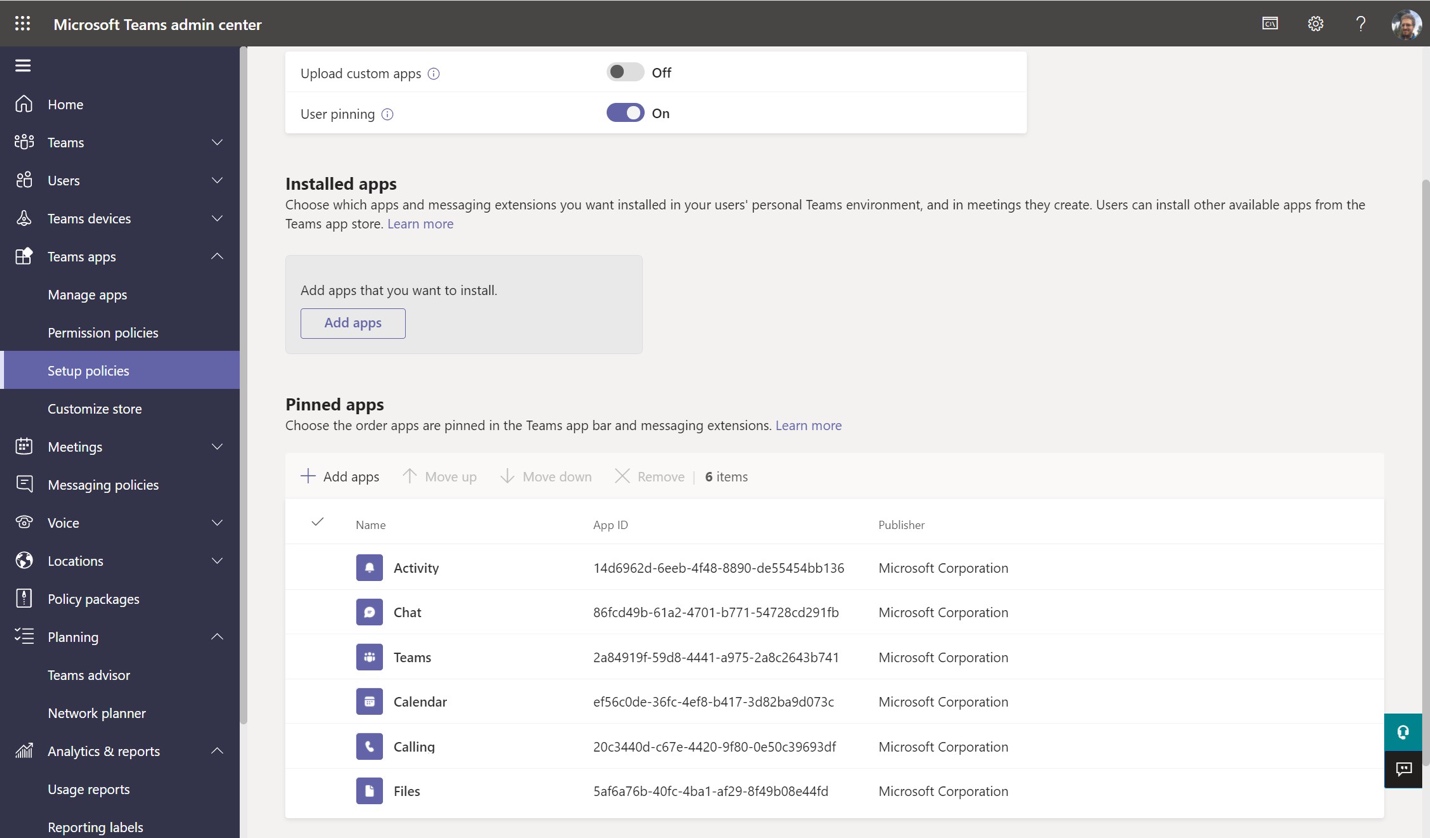
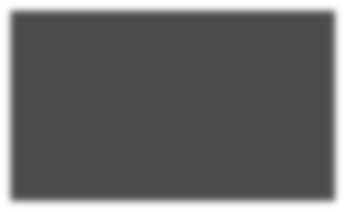
Remember that you can also mitigate risks with regard to third-party apps using **Admin consent requests** in Azure AD (see the Azure AD Best practices checklist).

Next, using **Permissions policies** you would be able to restrict who has the ability to install the approved apps, and whether to allow all apps and block specific ones, or block all apps but

allow specific ones.

© Copyright 2019-2022

11



Under **Setup policies**, you can choose which apps will be installed and pinned in the left navigation of the Teams app by default.

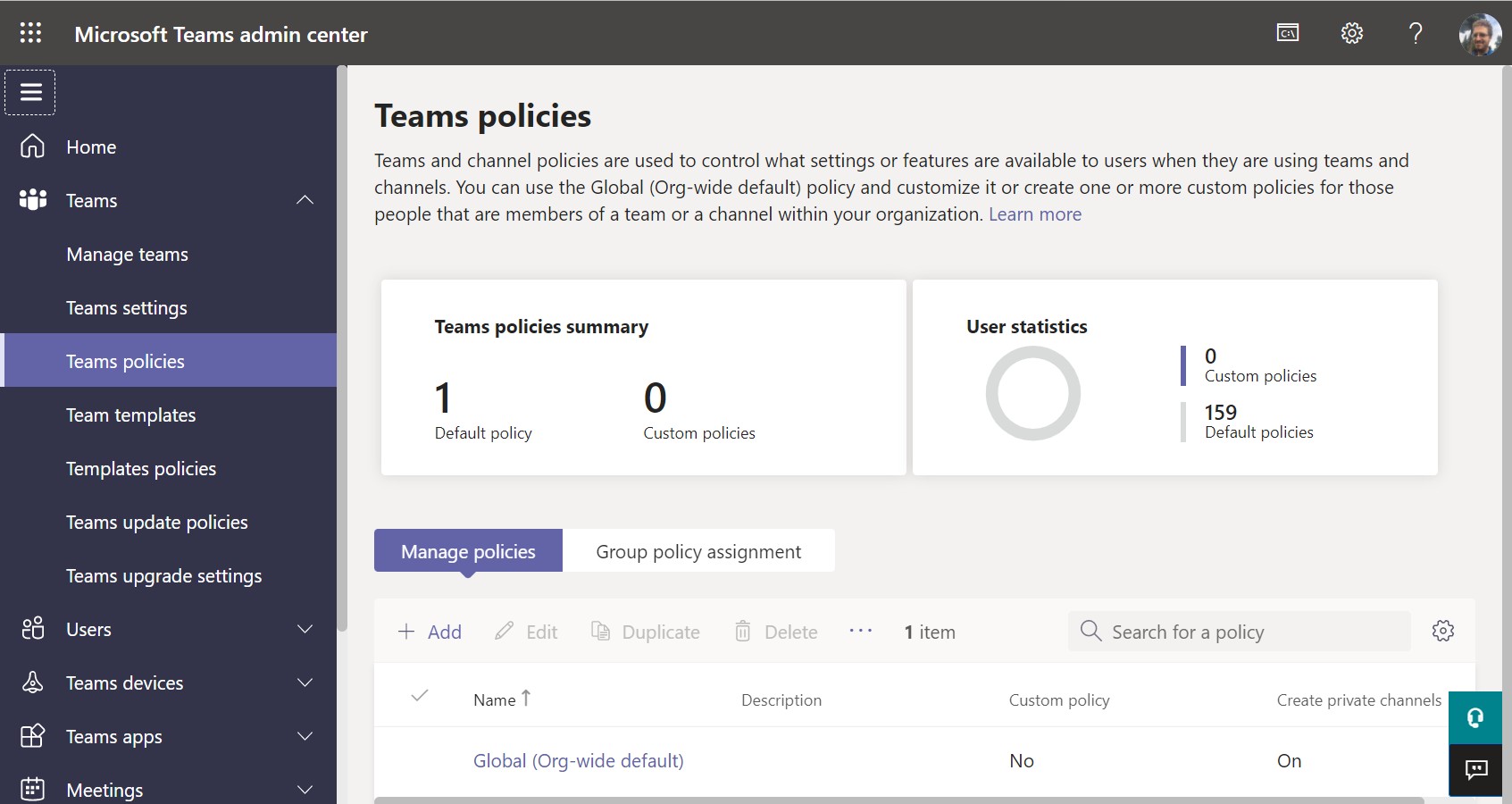
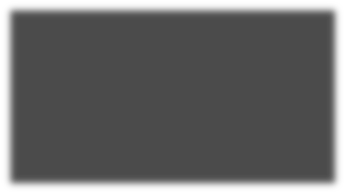
* **Enable or disable Private channels**

Private channels give users the option to create channels within a Team that are only visible to a sub-set of users within the Team. Choose whether **Private channels** are going to be allowed in

your organization; this can be configured from **Teams > Teams policies**.

© Copyright 2019-2022

12



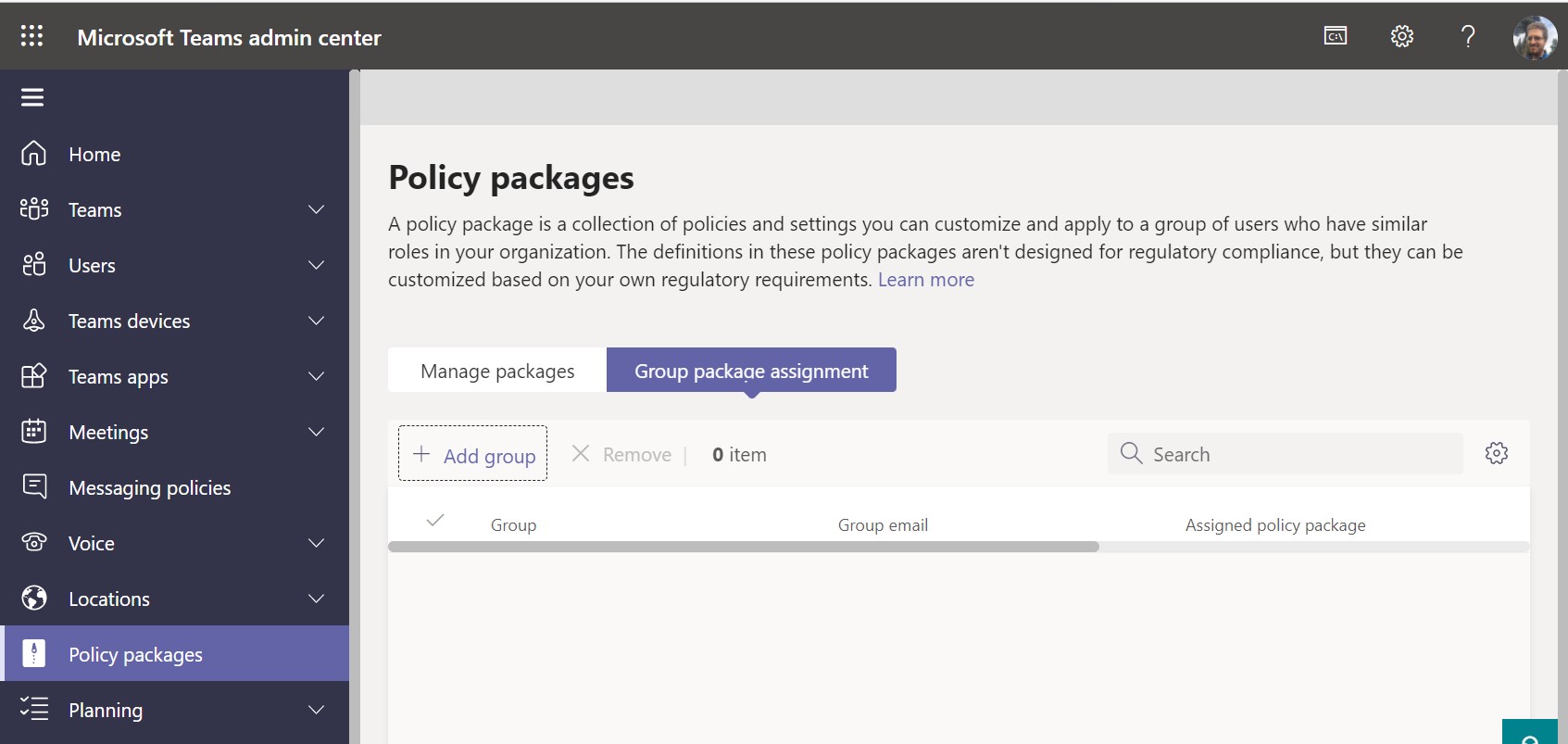
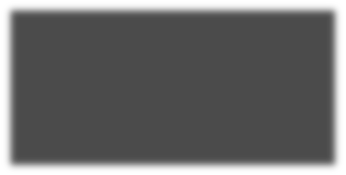
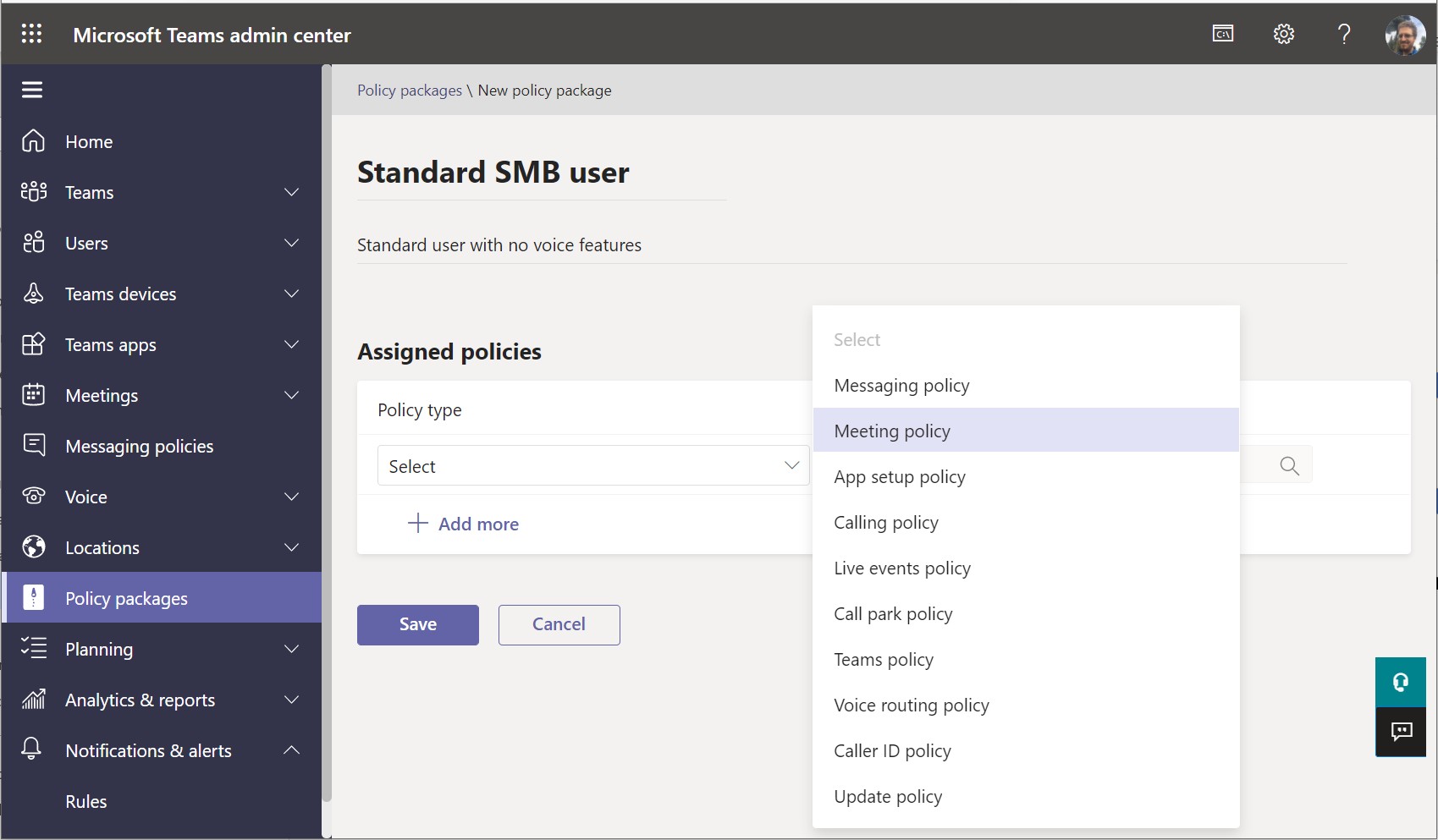
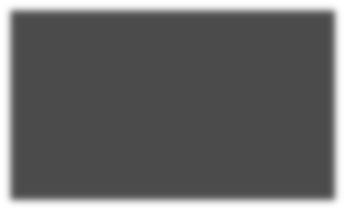
* **Using Policy packages**

You can use “**Policy packages**” from the left nav to configure and assign multiple policies at once to groups of users, which may be based on license type or job role. For example, you may have a different experience of the Teams app you want to present for frontline workers versus

standard users, versus users with voice features, etc.

© Copyright 2019-2022

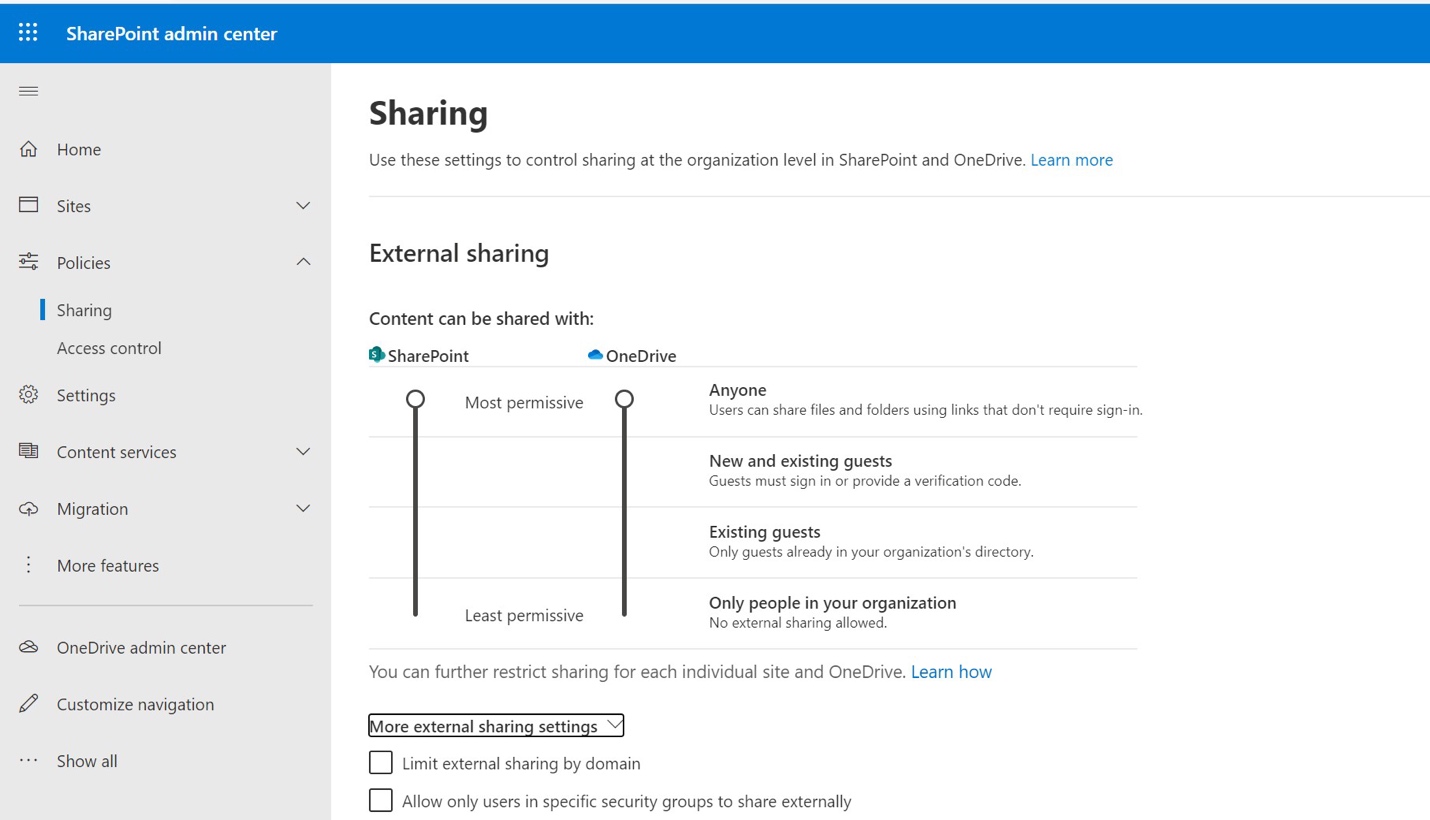
13



Once you have created your packages, you would assign them to groups under **Group package assignment > Add group**.

© Copyright 2019-2022

14



* **Global Sharing settings in OneDrive and SharePoint**

Review and adjust org-wide sharing settings to ensure they line up with the collaboration requirements for the org. Find these in the SharePoint admin center under **Policies > Sharing**.

For example, certain organizations will have a requirement to maintain an audit trail for all file access, which would imply that **Anyone** links must be disabled so that granting anonymous access to files is not possible. In that case you must move these sliders down to the **New and existing guests** selection. (However, be aware that disabling *Anyone* links also prevents you from using certain features such as [Request files](https://support.microsoft.com/en-us/office/create-a-file-request-f54aa7f8-2589-4421-b351-d415fc3b83af)). Also note that you cannot make your selection for SharePoint less restrictive than your selection for OneDrive.

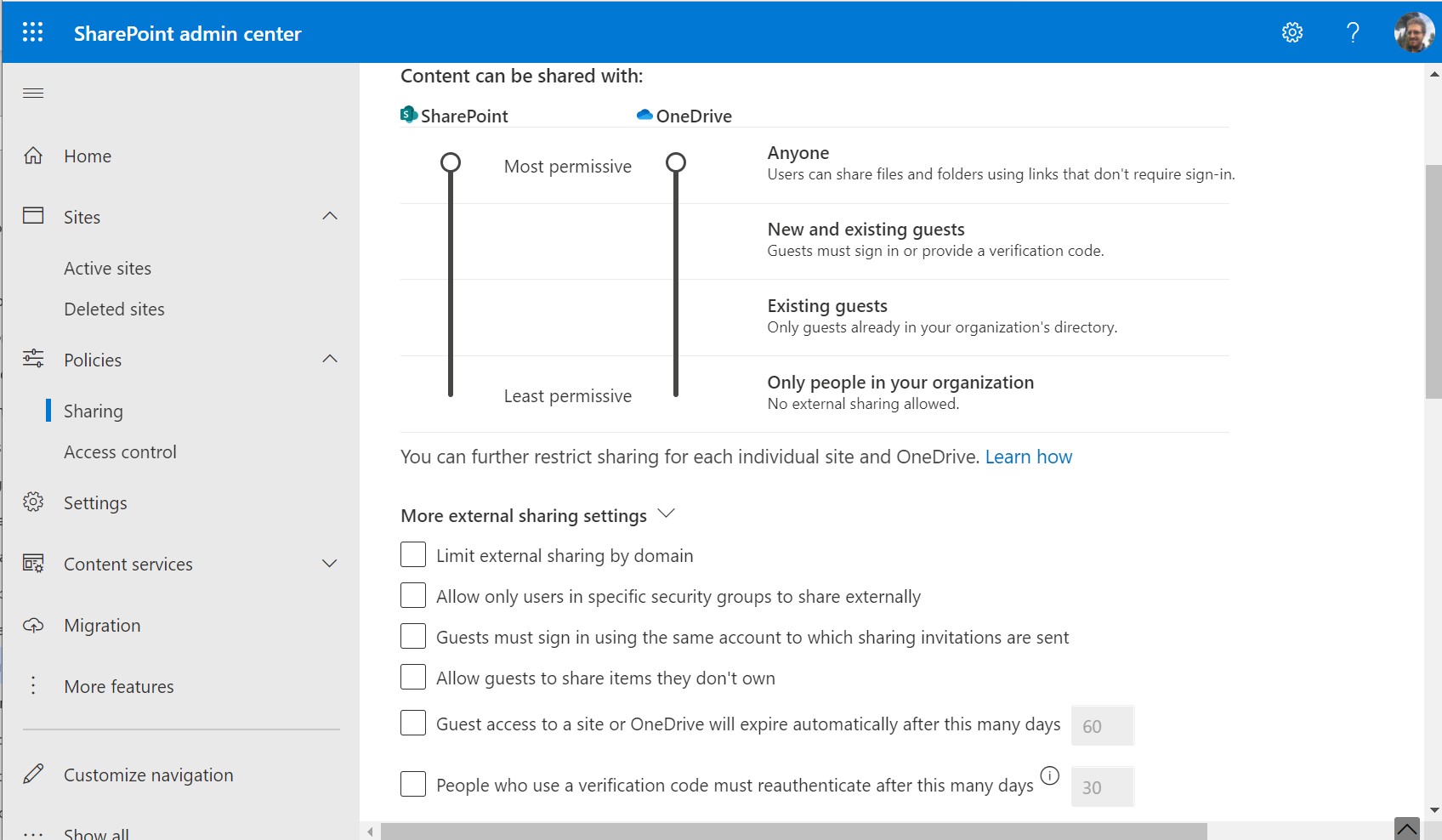
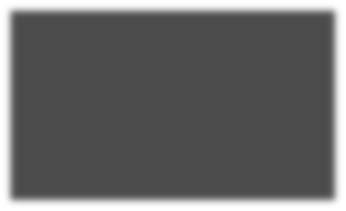
My personal best practice here is to leave this global setting on **Anyone** for both OneDrive and SharePoint. That way you maintain access to important features like **Request files**, and you would use other options for restricting link settings at the per-site level (also be aware that sites attached to Teams automatically do not allow *Anyone* links by default).

Next, be sure to review the options under **More external sharing settings**.

© Copyright 2019-2022

15

Unless you are required to disable **Anyone** links, recommend leaving them enabled for both OneDrive and SharePoint.



•

**Limit external sharing by domain**: You would only use this where an org has very specific partners with whom sharing is allowed

**Allow only users in specific security groups to share externally**: Use only where this special requirement exists. Some orgs may have “no external sharing” policies, with exceptions for specific functions in the business.

**Guests must sign in using the same account**…: This means guests must sign in using the email that you sent a sharing invitation to. So if they received it at a work account, they cannot sign in using a personal account to retrieve the content. A good option.

**Allow guests to share items they don’t own**: This option is enabled by default which think is a terrible default selection for most organizations. Generally, find that small business owners are okay sharing some content externally, but rarely do they want their invited guests to turn around and invite additional guests to that same content without their permission.

**Guest access to a site or OneDrive will expire automatically**…: This can be a good option for many businesses. Usually when content is shared externally, the idea is to enable temporary collaboration, not indefinite access. However, some may prefer to leave this disabled.

**People who use a verification code must reauthenticate**…: Leave disabled to allow

users who signed in with a code to stay signed in, or require they reauthenticate after a certain number of days.

•

•

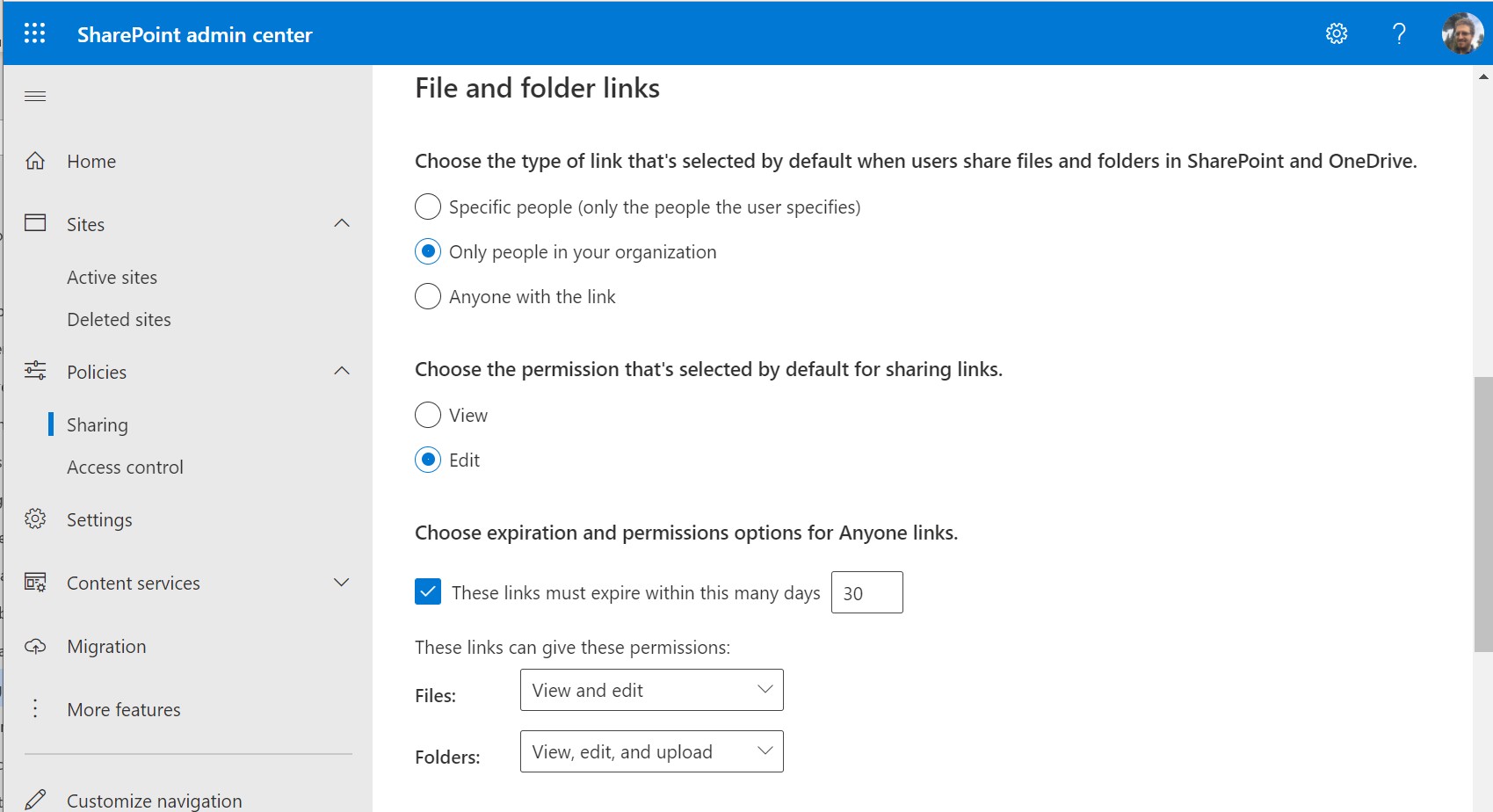
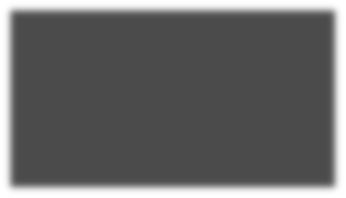
•

•

•

© Copyright 2019-2022

16



Scroll down and find some additional settings that you can use to control which type of link is selected by default when someone uses the “Share” button, as well as the permissions that are applied (users can always edit the selections themselves when sharing, so this just controls the *default* selections). As well, if you want to place an automatic expiry on “Anyone” links, you can

do that below.

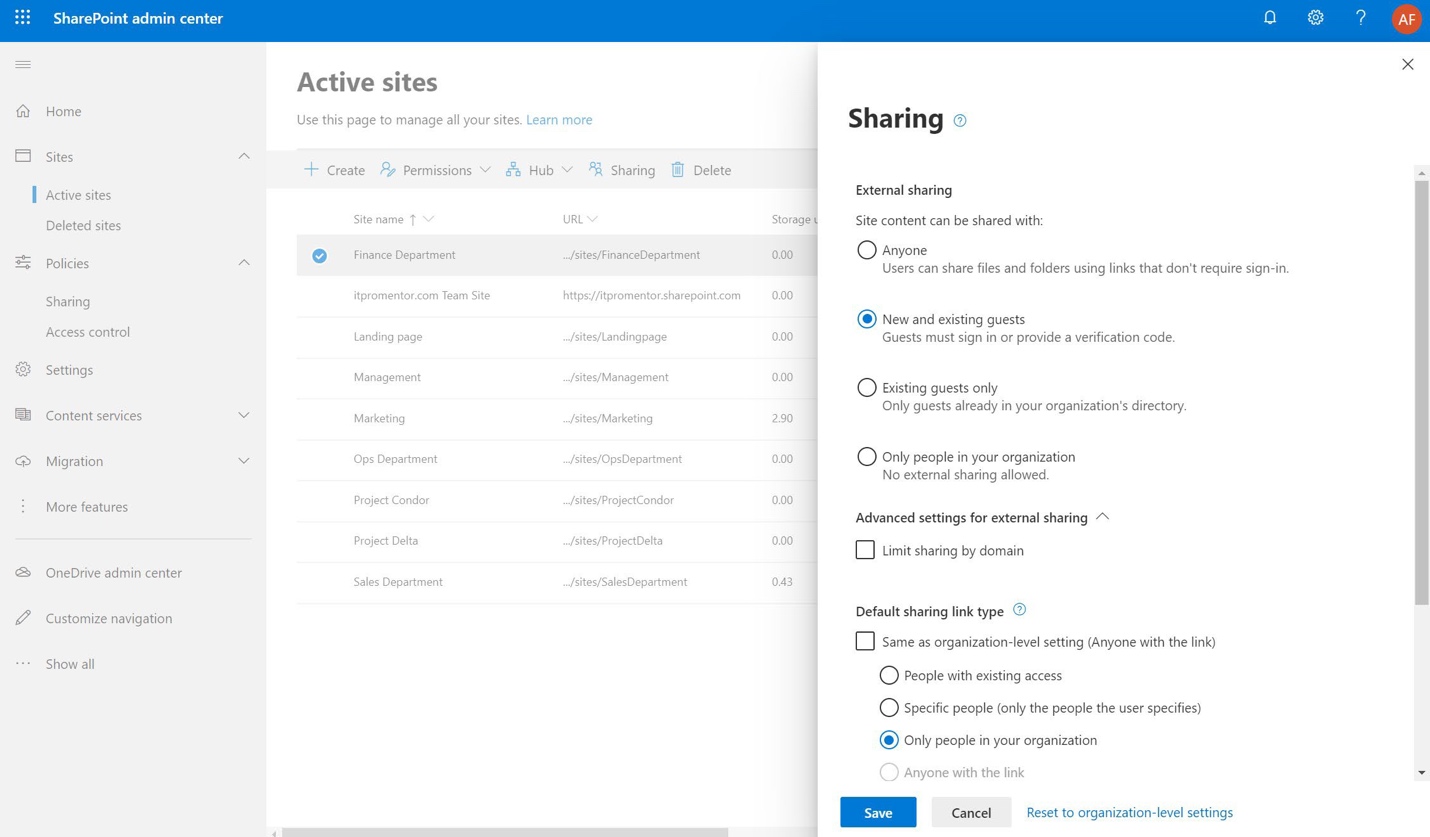
* **Site-level sharing settings**

If you choose to keep your **Anyone** links available at a global level, know that you can also restrict sharing on a per-site basis. Click any site under **Active sites**, and edit the **Sharing**

settings.

© Copyright 2019-2022

17



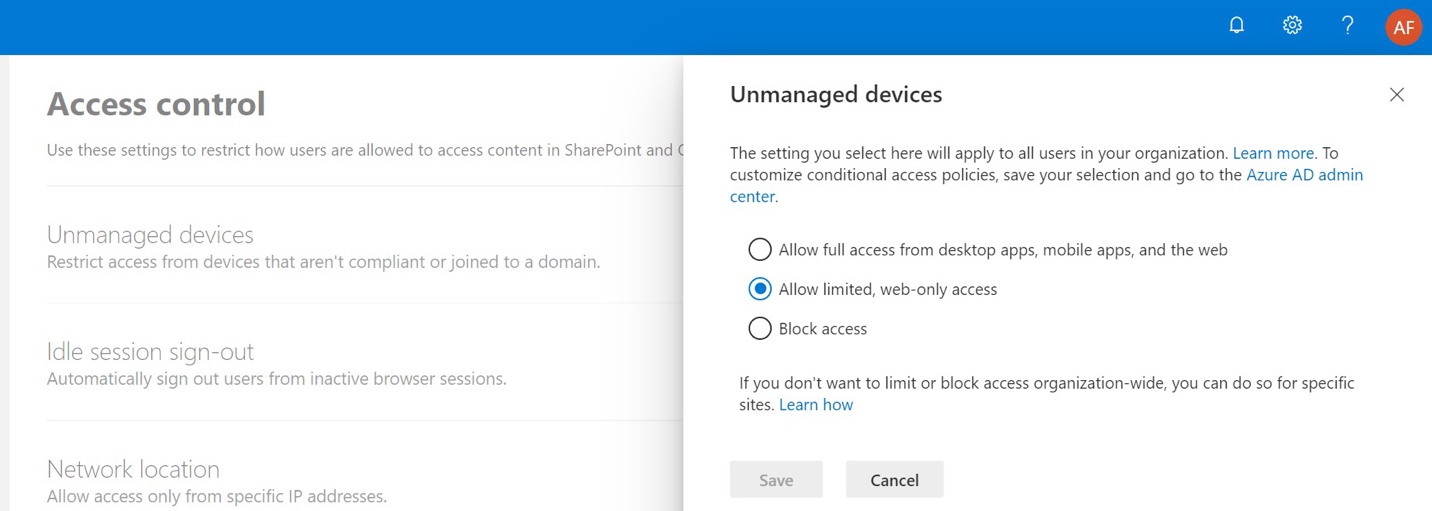
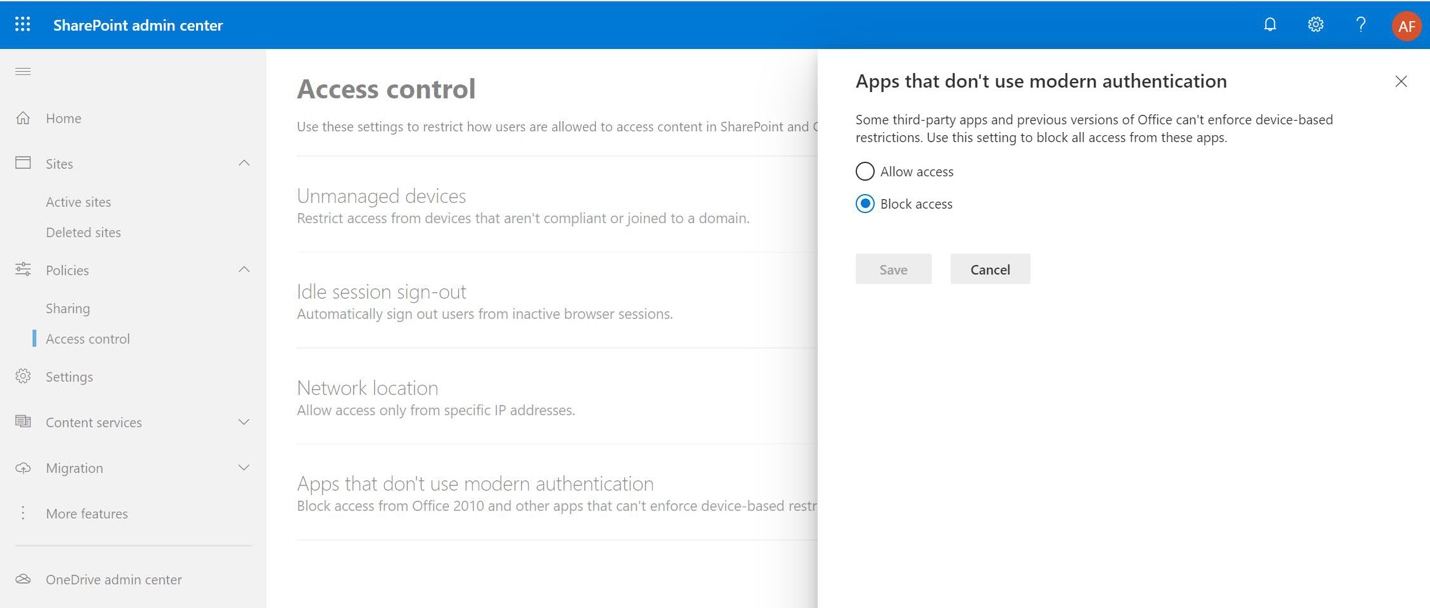
Also be aware that sharing settings can be controlled using Sensitivity labels when the labels are applied to Sites.

* **Customize Access Control for SharePoint Online and OneDrive for Business**

Review the settings under **Policies > Access Control**. At a minimum, you should Block access from **Apps that don’t use modern authentication**.

© Copyright 2019-2022

18



If you choose to enable the access controls for **Limited, web-only access** or **Block access** under

**Unmanaged devices**, be sure to see my Conditional Access best practices for more details.

•

**Allow full access**…: The default setting, which means that unmanaged devices have the same level of access as managed ones (full access).

**Allow limited, web-only access**: Unmanaged devices will not be allowed to download, print or sync information from SharePoint/OneDrive on their device, however browser access is allowed (Edge is supported but Firefox and Chrome will not work by default). **Block access**: Unmanaged devices will not be allowed access to OneDrive/SharePoint

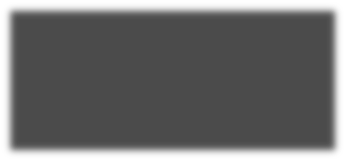
sites. You must have a device that is either compliant or Hybrid Azure AD Joined.

•

•

© Copyright 2019-2022

19



* **Use “Anchor” teams in Microsoft Teams**

Every organization that plans to use Microsoft Teams should start out with “Anchor” teams. The

Anchor teams are teams which are very well-defined and will persist for the foreseeable future in the business. For example:

**Org-wide team**: SMB organizations often have a pretty flat structure and tight-knit teams, with open collaboration atmospheres. In some cases, the org-wide Team will be the primary team for the company, with several different channels tracking different areas or functions within the business. In other cases, it may only be used for org-wide announcements. Either way, it tends to be useful, so it is always recommended to have at least one org-wide team.

**Department-wide teams**: Most organizations have divisions, business units, or departments that work together on common goals. For example, “Sales.” These teams often have a need to converse and share information about their “niche” within the business, and most of this conversation does not need to be exposed to other areas of the organization.

**Cross-department teams**: There may be some functions or repeatable business

processes which require their own Team.

•

•

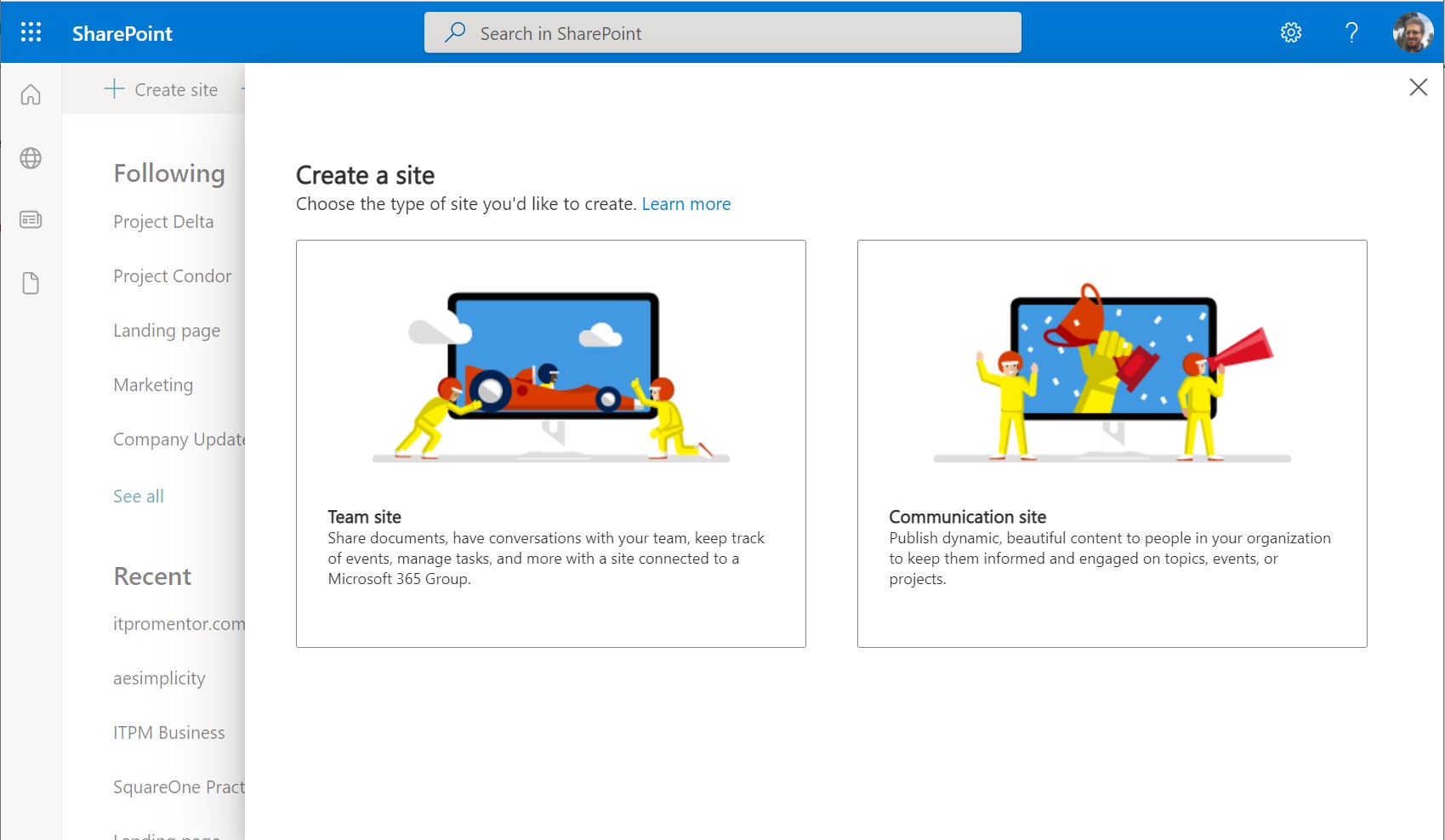
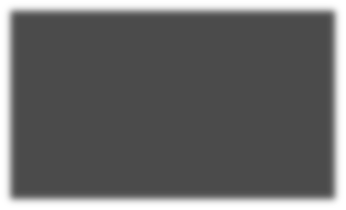
•

There may be other examples besides. But these are different than ephemeral teams which might be based on temporary projects, and eventually expire. recommend that when you have your “Anchor teams” established, you give them formal icons, good descriptions, and generally treat them with more professionalism: these should look like the “Official” channels of the

business.

© Copyright 2019-2022

20



* **Use Communication Sites for custom permissions**

While it is possible to manipulate site permissions for any SharePoint site, it is important that you do not attempt to modify the underlying permissions structure for sites which are tied to Microsoft 365 Groups (e.g., Teams). Instead, if you need to create a set of custom permissions,

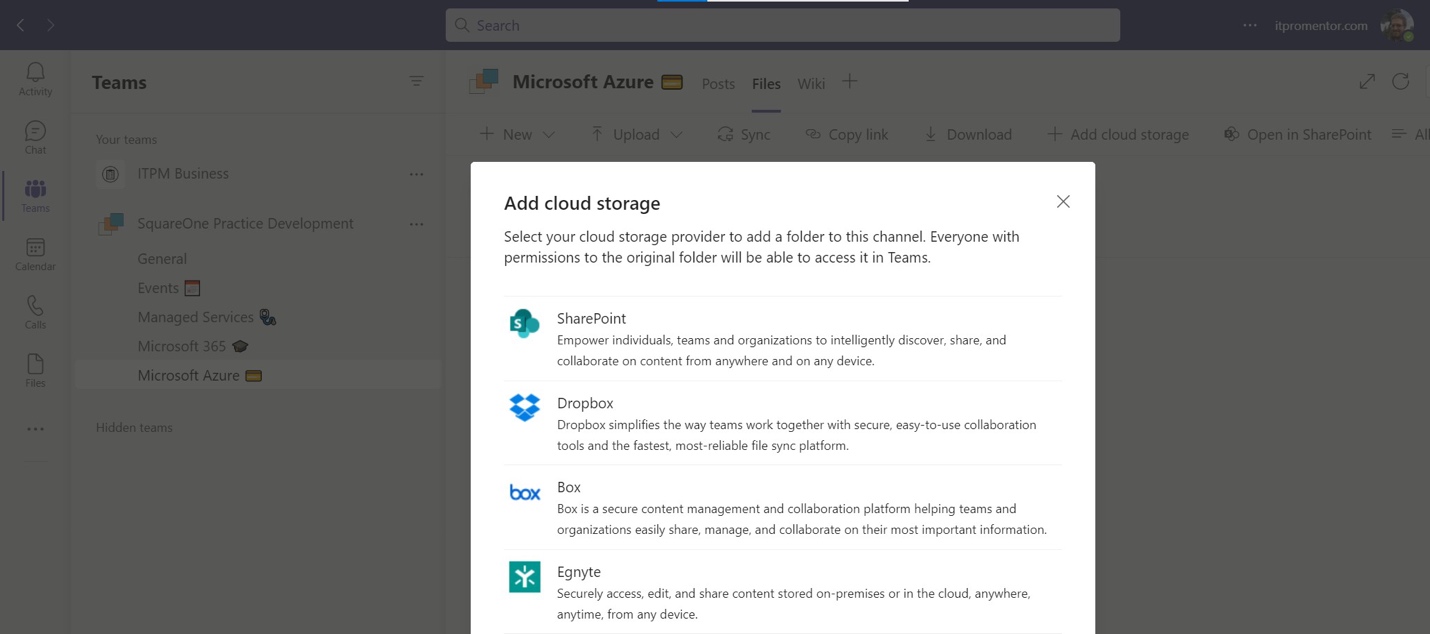
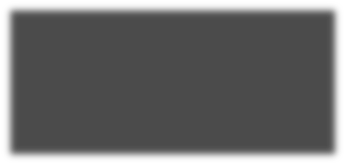
you should use a SharePoint Communication site.

For example, if you need to present content where some members have read-only access and some members have permissions to edit or modify the content, then you would use a Communication site for this purpose, not a Team site (which is the same type of site attached to teams inside the application Microsoft Teams). Team sites are connected to Microsoft 365 Groups, and by default the permissions structure on Teams sites is purposefully simplistic: every

member has edit/modify capabilities by design.

© Copyright 2019-2022

21



You can still present the content stored in Communications sites into a Team, for example you can **add a tab** into any given Teams channel, or even use the **Add cloud storage** to link to the

appropriate document libraries.

© Copyright 2019-2022

22